

# ROLE OF DATA PROTECTION LAWS IN ENVIRONMENTAL CONSERVATION: EXPLORING THE POSSIBILITIES AND CHALLENGES

<sup>1</sup> MADHAV SREEKUMAR <sup>2\*</sup> ABHINAV SHRIVASTAVA · <sup>3</sup>RAJ VARMA

<sup>1</sup> Student, Symbiosis Law School (SLS)

<sup>2\*</sup> Assistant Professor, Symbiosis Law School (SLS)

<sup>3</sup>Assistant Professor, Symbiosis Law School (SLS)  
Symbiosis International (Deemed University) (SIU),  
Vimannagar, Pune, Maharashtra, India

<sup>2\*</sup>Email: abhinavshrivastava1992@hotmail.com

## Abstract

*The globe is heading towards a digital future where data is an exploitable commodity. In these circumstances, data privacy is the need of the hour. This paper explores a positive side-effect of data privacy regulations. Regulations such as the GDPR have led to decreasing in pollution and energy consumption. These reductions are worth looking into. When they are projected on a global scale, the positive effects are magnified. The paper highlights the impact of big data centers on the environment and makes a case for a reduction in data collection, storage, and transmission. The paper also shows why data protection can be a good first step toward realizing the goal of environmental protection. Lastly, the paper looks at the Indian perspective on data protection and India's proposed plans for the future. India being a conventional fuel-dependent country stands to benefit greatly from the environmental effects of data privacy as well.*

**Keywords:** Data Privacy, Data Protection, Data Privacy GDPR, Conventional Fuel

## Table of Contents

### Introduction

1. The effects of big data on the environment
2. Data centers and their Impact on the Environment in India
3. The current state of Data Protection laws
4. The positive effects of Data Protection regulation on the environment

### Conclusion and the way forward

## Introduction

As the digital age has taken hold of the world and more of the world's population gains access to the internet, companies and other entities have found increasingly invasive methods of harvesting and exploiting their customers' data for monetary gain. Taking into account the exploitative nature of these practices, many governments have introduced or are planning to introduce regulations that protect their citizens' data from the clutches of companies and advertisers. These regulations have been shown to be highly effective in accomplishing the goal of protecting the data of citizens of cyberspace; however, there is a positive side effect of these regulations that accomplishes an even greater goal.

The effect of data protection regulations on the environment is a field that has not had much research. Since the implementation of the General Data Protection Regulation in the EU, its effects on the environment have come to light. From reducing energy usage to decreasing carbon emissions, the effects of the regulation have been numerous. The extent of the effect is worth exploring seriously as the presence of data and cyberspace become even greater parts of the human experience and the fields supporting this expansion get more power hungry and environmentally destructive.

This paper aims to explore the potentially useful effects of data protection regulation on the environment with a particular focus on the observable effects produced by the GDPR and the future of

such regulation in India and globally. It also aims to explore the way that big data has negative effects on the environment and how this can be mitigated.

### 1. The effects of big data on the environment

Energy consumption is one of the biggest concerns that is arising as a result of the growth of the IT field. The data centers and internet infrastructure required to maintain the global internet and all of the devices connected to it consume a staggering amount of energy in the form of electricity. In 2016 it took nearly 70 billion Kilowatt hours of electricity to run the internet<sup>1</sup>.

With the rapid growth of the field as connected devices get cheaper and more accessible in previously underdeveloped parts of the world this consumption is only expected to rise.

It is important to see how the industry uses energy and which parts of it can be minimized by effective data protection regulation. The major ways in which data uses energy is:

1. Electricity used by data center equipment for its operation.
2. Electricity is used to cool the equipment.
3. Energy is used to create the infrastructure and equipment.
4. Transportation of the equipment and other resources.
5. Employees/technicians travel for maintenance.

In a voluntary project with 184 participants, including companies like IBM, BT, HP, Vodafone, and Unilever as well as organizations in the public sector like the United Nations, the European Commission published a code of conduct for data centers in 2008. The objective was to make data centers more energy-efficient while also establishing a set of minimal voluntary criteria that may later be used as the foundation for more stringent regulation.

By 2020, it was projected that the energy used in data centers in Western Europe will increase by half, from 56 TWh to 104 TWh.<sup>2</sup> Electricity used by data centers in 2015 was 416.2 terawatt hours (2-3% of global energy consumption).<sup>3</sup> Total energy consumption by data centers is estimated to reach 14% of global energy consumption by 2040. The rise of data heavy processes such as video calling, cryptocurrency mining and user data farming will accelerate this increase in energy usage. Most of energy used by data centers is made using environmentally destructive methods such as fossil fuels. Virginia's "Data center alley", the site of 70% of the world's internet traffic (as of 2019) uses power from non-renewable energy sources.<sup>4</sup>

India relies heavily on coal and natural gas for its electricity production. This is especially true in the case of heavily industrialized states such as Maharashtra that is home to most of India's data centers. Therefore it becomes necessary to include this cost in energy production and pollution when addressing India's energy consumption and pollution goals and commitments. As part of COP26<sup>5</sup>, India has promised to achieve "net zero emissions" by the year 2070 and to bring its carbon intensity down to 45% by the year 2030. The positive environmental effects of data protection regulations can help to offset the rising carbon footprint of the IT sector in India and thereby help India to achieve its carbon goals.

A significant portion of energy consumed goes to keep storage and computing equipment cool. Equipment such as servers and hard drives which store data and house crucial digital infrastructure are extremely sensitive to temperature. High temperatures may affect the functions of these devices by either hindering performance or causing damage to them. These devices also generate waste heat during their functioning that accelerates their decline in performance. Data centers often use systems that use water or chemical coolants for cooling their server racks. Water is piped around the center to absorb the waste heat and then the hot water is expelled. This heated water is often piped into nearby

<sup>1</sup> C. Helman, *Berkeley Lab: It Takes 70 Billion Kilowatt Hours A Year To Run The Internet*, (2016) Forbes.

<sup>2</sup> *Establishing a code of conduct for data centres to improve energy efficiency*, (2016) World Economic Forum.

<sup>3</sup> T. Bawden, *Global warming: Data centres to consume three times as much energy in next decade, experts warn* (2016) Independent.

<sup>4</sup> G. Cook & E. Jardim, *Clicking Clean Virginia: The Dirty Energy Powering Data Center Alley*, (2019) Green Peace Reports.

<sup>5</sup> S. Mehta, *COP26 and Commitment of India*, (2022) 26 ENVIS RP: Geodiversity and Impact on Environment 3.



water bodies that can be harmful to the local ecosystems that are adapted to a particular temperature. Furthermore chemical coolants are often toxic in nature (CFC). HVAC systems used for cooling server rooms can account for as much as 50% of the energy consumed in a data center's daily operation<sup>6</sup>. There has been a push to move all data centers to areas with colder climates to decrease the need for overall cooling. However this introduces inefficiencies in transportation and maintenance. And is not possible in countries like India where the climate fluctuates throughout the year and the IT hubs are located in hot climates such as Mumbai, Bangalore and Delhi.

Devices such as hard drives and servers use precious metals like gold. The mining of these resources requires energy and causes carbon emissions. Furthermore mining of these materials often cause environmental destruction to the areas surrounding the mines in the form of deforestation, soil contamination and water contamination.

A big problem that is being faced following the explosion in popularity of devices is E-waste generation. E-waste is generated as equipment fails. In India the E-waste generated in this manner would be regulated under the E-Waste (Management) Rules, 2016<sup>7</sup>. Equipment used in digital infrastructure that is constantly being used to maintain and store data has the potential to fail even more than consumer devices due to their increased and constant usage. A large amount of E-waste is generated in this manner. Components like batteries use toxic and dangerous material like lithium (flammable). The disposal of potentially toxic and dangerous materials found in batteries would also come under the E-Waste (Management) Rules, 2016.

Some data centers are located in colder regions to decrease cooling requirements. However these are often in harder to reach places. This means an increase in the carbon footprint of technicians that have to travel to and from these data centers. There is also increased energy usage and emissions from building and maintaining large data center facilities. This includes on-site power back-up generators, transportation of supplies, and heating and cooling the buildings in general.

To make sure that no data is lost and to ensure that data is available at a moment's notice across the globe, there are multiple instances of the same data stored in different locations for redundancy. There may even be multiple instances of data stored in the same data center or even the same storage rack. This effectively doubles the energy used by the same data.

The Climate Neutral Data Center Pact<sup>8</sup> is an agreement between major players in the data sector in the EU to become climate neutral by 2030. This is to be done by adopting clean energy providers, more efficient processes, better management and using renewable energy. There is also research that is being done to make data centers greener<sup>9</sup>. There have been talks to adopt the features of this agreement and other research into a comprehensive policy under the GDPR.

## 2. Data centers and their Impact on the Environment in India

In states with the largest number of data center projects, namely Maharashtra and Delhi NCR, some 78% and 85-90% of the total electricity generated is from fossil fuel sources, and mostly coal. Maharashtra alone hosts more than 40% of India's installed data centers. Further, Maharashtra has projects which will double its installed capacity by 2023. It seems unlikely that this expansion can be achieved without serious reliance on coal and fossil fuel-powered electricity.

2020 saw India's draft 'National Data Centre Policy'<sup>10</sup> Several large states have also announced their data center policies and signed MoUs with private players to create them. India's data center capacity is expected to double from 499 MW in 2021 to 1,008 MW by 2023. The draft speaks about economic and technological development and expansion in this field however it does not talk about the potential

<sup>6</sup> M. Dayarathna, Y. Wen & R. Fan, Data Center Energy Consumption Modeling: A Survey, (2016) 18 IEEE Communications Surveys & Tutorials 1.

<sup>7</sup> E-waste (Management) Rules, 2016, G.S.R. 261(E), Acts of Parliament, 2016

<sup>8</sup> *Climate Neutral Data Centre Pact*, Climate Neutral Data Center.

<sup>9</sup> X. Jin, F. Zhang, A. Vasilakos, Athanasios & Z. Liu, Green Data Centers: A Survey Perspectives, and Future Directions, (2016) arXiv.

<sup>10</sup> Data Centre Policy, No. xxx/YY/2020, Ministry of Electronics & Information Technology (e-Governance Division)

environmental impact or mitigation strategies. It does seek to encourage the use of clean and renewable energy in the form of solar power, wind power and hydroelectric power.

One of the biggest resources used by data centers is water for cooling as well as maintenance. A NITI Aayog report<sup>11</sup> predicts water crises in Mumbai, Bengaluru, Delhi, and Chennai which are the major IT hubs of India and home to most of India's data centers. Furthermore, there is concern that the waste hot water that is expelled by data centers as part of its cooling measures may lead to ecological damage in the water bodies near these centers. Water pollution is a huge problem in India and the ecological damage caused by the temperature of water bodies rising will make this problem worse as entire ecosystems based on the water body collapse.

### 3. The current state of Data Protection laws

In the European Union, General Data Protection Regulation (GDPR)<sup>12</sup> unifies data protection laws. It went into effect on May 25, 2018. This law focuses on the transparency of business regarding the collection and storage of user data. The law is based on the philosophy that personal data must be protected against "unauthorized or unlawful processing, and against accidental loss, destruction or damage." According to the provisions in this regulation data collected must be specific and for a legitimate purpose and shouldn't be used in any way beyond that intention. Also, data should be limited to what is necessary in relation to the purposes for which they are processed. The GDPR influenced the creation of data protection laws in other parts of the world such as the California Consumer Privacy Act (CCPA) which is expected to lead the charge in the creation of a nationwide data protection law in the United States and the Law on the Protection of Personal Data No. 6698 dated April 7, 2016 (LPPD) which is the Turkish data protection regulation.

In the USA, the California Consumer Privacy Act (CCPA)<sup>13</sup> will likely lead the charge for the US to create a federal data protection regulation. As one of the most important centers of digital traffic and the home of major companies such as Google and Microsoft that deal with the data of billions of users across the world, it is imperative that the US create proper data protection laws to ensure there is a check placed on these big tech giants.

In China, the Personal Information Protection Law (PIPL)<sup>14</sup> in addition to bringing all of China's data privacy regulations under a single roof, introduces a number of noteworthy innovations to the country's system for protecting individuals' private information. Among them are the imposition of hefty penalties, extraterritorial application, the need of data protection officers, and the establishment of new laws controlling the flow of data across international borders. The PIPL will strengthen the new rights that data subjects who reside in China have obtained, regardless of their nationality, such as the right to have their data deleted and the right to withdraw their permission for data collection. Companies that handle a significant amount of personally identifiable information will be obliged to hire a data protection officer who will be responsible for overseeing the organization's data management practices. In accordance with the PIPL, the processing of sensitive personal information across international boundaries will be subject to a threshold. Should it be exceeded, a corporation will be required to localize the data processing operations it carries out.

In Australia, the Review of Privacy Act, 1998 and the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Online Privacy Bill)<sup>15</sup> are being reviewed by the Australian Government to include new frameworks for digital application. The review aims to look at the reach and application of the Privacy Act; whether or not the Privacy Act offers a framework that is both realistic and adequate for encouraging appropriate privacy procedures; whether or not the Privacy Act

<sup>11</sup> *Composite Water Management Index, (2019) NITI Aayog,*

<sup>12</sup> REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

<sup>13</sup> S. Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA) (2018)* 33 *Berkeley Technology Law Journal* 1.

<sup>14</sup> C. Blanton, *China's Personal Information Protection Law (PIPL) (2021)* The University of Texas System.

<sup>15</sup> Attorney-General's Department, *Review of the Privacy Act, 1988, Australian Government*

effectively protects personal information; It also seeks to answer jurisprudential questions such as if individuals should have direct rights of action to enforce privacy obligations under the Privacy Act, if a statutory tort for serious invasions of privacy should be introduced into Australian law. The review also aims to examine the efficiency of the enforcement authorities and procedures provided by the Privacy Act, as well as how such powers and mechanisms interact with other regulatory frameworks within the Commonwealth. The Online Privacy Bill will introduce a binding Online Privacy code for social media and certain other online platforms. It will also increase penalties and enhance enforcement measures.

In Brazil, the Lei Geral de Proteção de Dados (LGPD)<sup>16</sup> is a data protection regulation that applies to all persons and legal organizations, public and commercial, that handle personal data about Brazilians, sell products or services in Brazil, or gather personal data in Brazil. It has extraterritorial reach, therefore no matter where a data collector is based if they collect Brazilian citizen data, they are subject to the LGPD. Personal data processing, journalistic, artistic, literary, academic, or national security, defense, public safety, criminal investigation, or punishment is excluded from LGPD compliance. All companies subject to the LGPD must establish a Data Protection Officer (DPO) to operate as a liaison to Brazil's data protection authority, the Autoridade Nacional de Proteção de Dados (ANPD), process complaints, and give compliance and best practices recommendations. They must also take technological and administrative steps to secure personal data against unauthorized access, loss, modification, transmission, and distribution. They must also perform Data Protection Impact Assessments (DPIA) and prepare a reaction and repair strategy. LGPD requires breach notification. If a data breach poses a danger or harm to data subjects, companies must notify the ANPD and, if mandated, the affected data subjects and the media. Under the LGPD, data subjects may request that their data be updated, destroyed, or supplied in a readily accessible format that can be transferred to a different firm. They must also be notified of the reason for which data is being gathered. Companies must develop processes to handle data subject requests. They must also destroy data once it's no longer required for the original purpose unless they receive data subjects' explicit permission.

In India at present, data protection in India dependent on Information Technology Act, 2000 read with provisions of the IPC and CrPC. This approach does not directly address personal data that act as identifiers such as name, identifiable numbers etc. No framework exists in India for controlling the data collected by businesses. The Personal Data Protection Bill, 2019 that was recently withdrawn from Parliamentary discussion aimed to introduce provisions controlling the flow and usage of personal data, protecting the collected data, ensuring accountability in cases of breach and creating remedies for those affected by such breaches. The Personal Data Protection Bill also aimed to establish a Data Protection Authority in India akin to the requirement of a state data protection authority in the GDPR. The Personal Data Protection Bill had been in the state of review for years without an end in sight. The delay has become a significant issue as in the meantime, India has witnessed a number of data privacy violations. IRCTC had a massive data leak<sup>17</sup> in 2020 which led to the data including full names, numbers, emails, date of birth and city of residence of around a million users being leaked. Air India's passenger system service provider also had a data breach<sup>18</sup> which led to the leak of even more sensitive data such as credit card information and passport information of around 45 Lakh users. These leaks further demonstrate the need for data protection regulations in India. The data found from these leaks can be used for the purposes of propagating spam emails and calls and in phishing and social engineering scams. And these and lead to further hacks of end user accounts which is particularly dangerous when credit card information is involved. Therefore not only do these holes in data security cause unnecessary stress on India's developing network infrastructure, it also leads to scams and other cyber-crimes. The withdrawal of the PDPB is a devastating roadblock in the road to the creation of an effective data protection regime in the country.

<sup>16</sup> A. Coos, *Brazil's LGPD is now in effect*, (2020) End Point Protector.

<sup>17</sup> HT Tech, *User data of more than 900,000 leaked from IRCTC last year, resurfaces on the dark web*, (2022) Hindustan Times.

<sup>18</sup> *Incident Report: The Air India and SITA PSS Data Leak*, (2022) CyberPeace foundation,



#### 4. The positive effects of Data Protection regulation on the environment

Following the GDPR coming into effect, some websites are noted to load faster. Ads and data trackers made up 91% of the size of a website in some cases.<sup>19</sup> Not using trackers and targeted ads can reduce time taken to load a website, data stored in website servers, energy required to send and receive data from users leading to overall reduction in energy consumption and emissions.

There has been a drastic reduction in marketing emails as advertisers do not have access to this data and therefore cannot send emails to bulk email lists. The number of emails sent for advertising was reduced by as much as 1.2 billion per day.<sup>20</sup> This has led to a reduction of 360 tonnes of CO2 emissions per day. (Average CO2 emission per email (75kb average size<sup>21</sup>) is 0.3g<sup>22</sup> |  $0.3 \times 1.2 \text{ billion emails} = 360 \text{ tonnes of CO2}$ )

1.2 billion emails at 75kb per email is about 90 terabytes of data stored on email servers, transferred across the internet and displayed on user devices. This leads to energy consumption, need for more storage (resulting in more mining for metals and other resources for storage devices), more CO2 and other pollutants from data centers.

The GDPR has clearly resulted in reduced carbon emissions and reduced energy consumption in the EU. However the environmental benefits of data privacy laws will be multiplied when applied on a global scale. According to a study<sup>23</sup> conducted by McAfee and ICF international there are an estimated 62 trillion spam emails sent every year consuming close to 33 billion kilowatt-hours(KWh). These emails are sent in bulk to email lists compiled from user data sold by companies to advertisers and scammers. The annual global energy required for creating, sending, receiving, storing, and viewing spam is more than 33 billion KWh, comparable to four huge new coal power plants. ICF estimates spam-related emissions for all email users at 17 million metric tonnes of CO2, or 0.2% of global emissions.

Spam emails account for close to 80% of all emails sent globally. National data protection regulations are essential to reduce the number of emails that can be farmed by companies and sold to advertisers. Such a reduction is monumental in reducing the carbon footprint as well as the energy consumption by the process of sending spam emails.

Reduction in spam is only one of the benefits of data privacy regulations. As observed in the EU, better regulation of website trackers will lead to less data heavy websites. Trackers are pieces of code that observe user activity that are embedded in websites in order to learn about a user and then use that information to serve specifically targeted advertisements to that user. There can be multiple trackers on a website which leads to larger websites that take up more space on a server and takes more time to load and more energy to maintain and view.

As of October 2021, India is the 5th most spammed country in the world with an average of 7.97 billion spam emails sent per day<sup>24</sup>. This amounts to approximately 2391 tonnes of CO2 emissions per day. India is also 4th in the world when it comes to spam calls<sup>25</sup>. These spammers get information about emails and phone numbers from companies that sell this user data to them for advertising purposes. The low technology literacy in India leads to users more voluntarily giving up their user data when asked by companies. The users are unaware of the ways in which their data is being used for advertising and spamming. Considering the right to privacy that India holds to high regard this is unacceptable.

The way to reduce this is by implementing data privacy regulations that protect user data and limit the data that can be collected by companies. Similar provisions to the GDPR such as limiting data to only that which is needed for the company to provide their services and only using that data for their stated purpose will go a long way in combating this spam problem. The Personal Data Protection Bill, 2021 had proposed several such provisions that regulate collection. Post the implementation of this bill data

<sup>19</sup>James KIELTY, *Surveillance capitalism is killing the web*, (2018) MobiForge.

<sup>20</sup>C. Cimpanu, *Number of Third-Party Cookies on EU News Sites Dropped by 22% Post-GDPR*, (2018) Bleeping Computer.

<sup>21</sup>H. Tschabitscher, *Why Are Email Files so Large?* (2021) Lifewire.

<sup>22</sup>*What's the carbon footprint of ... email?* (2010) The Guardian.

<sup>23</sup>*The Carbon Footprint of Email Spam Report* (2011) ICF International&McAfee.

<sup>24</sup>*Daily number of spam emails sent worldwide (2021)* Statista.

<sup>25</sup>*Trucaller Insights: Top 20 Countries Affected by Spam Calls (2021)* Trucaller,

could only be collected to an extent that is reasonable and only for the purpose stated by the collector. The data subjects were to be given many rights over the collected data such as the right to delete the data whenever they want.

The proposed Digital Personal Data Protection Bill, 2022 is a step forward for India, however the provisions and effectiveness of this bill and the environmental effects of this regulation remain to be seen however since it is based on and will emulate the GDPR it is likely that there will be similar environmental benefits. The benefits may be more than the GDPR since India uses more non-renewable energy sources for its IT sector. It will also be beneficial for India's poor infrastructure for E-waste management. In the years 2019 and 2020 only 22.7% of the E-waste generated in India was collected, recycled or disposed of<sup>26</sup>. The rest of the E-waste remains in landfills and water bodies. The harmful pollutants found in components like hard drives contaminate soil and water bodies. Reduction in E-waste brought about by data privacy regulations will alleviate the stress on India's E-waste management infrastructure.

### Conclusion and the way forward

The importance of data protection regulation has increased in the modern day. Companies and advertisers seek to gain from misusing the data of their customers without consequence. Therefore it is important for governments to take steps to minimize the data that can be collected from their citizens that may not be aware of the way these companies are using their data.

As demonstrated by the GDPR these regulations are effective for their intended purpose, but they also have the useful side-effect of helping the environment. Data storage and transmission is a large consumer of energy and other resources as well as being polluting in nature. Companies selling data to advertisers leads to billions of spam emails and calls each day resulting in a huge wastage of energy required in the processes behind these systems. Applying the same standards for data privacy on a global scale would result in massive improvement in pollution, E-waste and energy savings. This is set to improve as technology advances and the amount of data created increases drastically in the future. Storage and transmissions require the use of equipment whose creation and maintenance consume even more resources in the form of precious metals and cooling energy. And this equipment becomes an E-waste problem once they reach the end of their service life.

In a country like India which has a huge spam and E-waste problem as well as being highly dependent on non-renewable, polluting sources of electricity, the decrease in data storage and data processing resulting from data protection regulation can be a huge boon. The proposed Digital Personal Data Protection Bill is a step in the right direction for both data protection in India as well as making the field of data collection, storage and transmission less environmentally destructive. The best way forward is if an environmental perspective is also considered by the framers of this bill and limits on collection and storage are developed to further environmental goals as well.

It is therefore becoming obvious that data protection regulation is the need of the hour for both, the right to privacy as well as to offset the environmental damage being caused by the ever-expanding Information Technology industry.

### References

- Attorney-General's Department, Review of the Privacy Act, 1988, Australian Government*  
*C. Blanton, China's Personal Information Protection Law (PIPL) (2021) The University of Texas System.*  
*C. Helman, Berkeley Lab: It Takes 70 Billion Kilowatt Hours A Year To Run The Internet, (2016) Forbes.*  
*Cimpanu, Number of Third-Party Cookies on EU News Sites Dropped by 22% Post-GDPR, (2018) Bleeping Computer.*  
*Climate Neutral Data Centre Pact, Climate Neutral Data Center.*  
*Composite Water Management Index, (2019) NITI Aayog,*  
*Coos, Brazil's LGPD is now in effect, (2020) End Point Protector.*  
*Daily number of spam emails sent worldwide (2021) Statista.*

<sup>26</sup> R. Jadhav, Around 78% of India's e-waste is not being collected or disposed by the government (2022) The Hindu BusinessLine.



*Data Centre Policy*, No. xxx/YY/2020, Ministry of Electronics & Information Technology (e-Governance Division)

*Establishing a code of conduct for data centres to improve energy efficiency*, (2016) World Economic Forum.

*E-waste (Management) Rules*, 2016, G.S.R. 261(E), Acts of Parliament, 2016

G. Cook & E. Jardim, *Clicking Clean Virginia: The Dirty Energy Powering Data Center Alley*, (2019) Green Peace Reports.

H. Tschabitscher, *Why Are Email Files so Large?* (2021) Lifewire.

HT Tech, *User data of more than 900,000 leaked from IRCTC last year, resurfaces on the dark web*, (2022) Hindustan Times.

*Incident Report: The Air India and SITA PSS Data Leak*, (2022) Cyber Peace foundation,

James Kielty, *Surveillance capitalism is killing the web*, (2018) MobiForge.

M. Dayarathna, Y. Wen & R. Fan, *Data Center Energy Consumption Modeling: A Survey*, (2016) 18 IEEE Communications Surveys & Tutorials 1.

of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

R. Jadhav, *Around 78% of India's e-waste is not being collected or disposed by the government* (2022) The Hindu Business Line.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

S. Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)* (2018) 33 Berkeley Technology Law Journal 1.

S. Mehta, *COP26 and Commitment of India*, (2022) 26 ENVIS RP: Geodiversity and Impact on Environment 3.

T. Bawden, *Global warming: Data centres to consume three times as much energy in next decade, experts warn* (2016) Independent.

*The Carbon Footprint of Email Spam Report* (2011) ICF International & McAfee.

*Trucaller Insights: Top 20 Countries Affected by Spam Calls* (2021) Trucaller,

*What's the carbon footprint of ... email?* (2010) The Guardian.

X. Jin, F. Zhang, A. Vasilakos, Athanasios & Z. Liu, *Green Data Centers: A Survey Perspectives, and Future Directions*, (2016) arXiv.